Security Implications of Cloud Computing

Doc Shankar
IBM Distinguished Engineer
Federal CTO Office
dshankar@us.ibm.com

Myths or Realities?

- Cloud is not as secure as a traditional IT operation
- Security patching is better in a cloud
- Demonstrating compliance is harder in a cloud
- Data loss is less likely in a cloud
- More control leads to better security
- Cloud providers can handle insecure apps better
- Cloud providers have a better view of threats
- Cloud offers more availability than in-house IT
- Cloud providers are more concerned with protecting themselves than the client

Agenda

- **Part I - Cloud Computing (CC) Overview**
  - A Simple Definition
  - A Complete Definition
  - Security Implications
- **Part II – Is CC New?**
  - Distributed Systems Evolution
  - Security Pain Points
  - CC vs SOA
  - CC vs Outsourcing
  - CC vs SaaS
- **Part III - Cloud Computing Security**
  - Customer Security Concerns
  - How do we get attacked?
  - Security Benefits
  - Security Risks
  - Security Issues

A Simple Definition of Cloud

Cloud is really about moving computing workloads off premise and delivering them as a “anytime, anywhere” service.

The hope is that, it more cost effective then traditional IT.

Historical Analogy

In 1907, 70 percent of the industrial electrical generation in the United States was in-house, but by the 1920s that same percentage was generated by utility companies. Initially you had to own your own plant, but later it became a disadvantage.

A Complete Definition of Cloud*

- Cloud Computing is a (**pay-per-use)** model for enabling **convenient, on-demand** network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be **rapidly provisioned and released** with **minimal management effort** or service provider interaction

* NIST Definition – Still an evolving paradigm; e.g. pay-per-use deleted

Delivery Models

- Software as a Service (SaaS)
  - Use provider's applications
  - Access through thick/thin clients, Browser, etc.
  - E.g. email, google docs, Sales force CRM, Desktop Apps.
- Platform as a Service (PaaS)
  - Deploy client applications using programming languages, tools supported by provider
  - E.g. MS Azure, Google app engine, Force, Amazon SimpleDB
- Infrastructure as a Service (IaaS)
  - Rent processing, storage, networks and other fundamental computing resources
  - Deploy arbitrary software including operating systems
  - Client could select networking components (firewalls, load balancers)
  - E.g. Amazon EC2, S3, Terremark, Rackspace

Security Implications of the Delivery Models

Service	Security by Cloud Provider	Extensibility
SaaS	Greatest	Least
IaaS	Least	Greatest
PaaS	Middle	Middle

The lower down the stack the cloud provider stops, the more security you are tactically responsible for implementing and managing yourself

Top Security Threats/Concerns

- SaaS (All (almost) concerns handled by provider)
  - Weak authentication credentials
  - Insecure protocols
  - Web-based application flaws
- PaaS (Consumers secure the applications)
  - Default application configurations (e.g. LAMP)
  - SSL protocol & implementation flaws
  - Insecure permissions on cloud data
- IaaS (Consumers secure the applications + OS & Services)
  - Caused by vulnerabilities in OS & services
  - MAC-based OS will contain the damage (least privilege principle)
  - Different mitigation strategies for OS & services; 3 options
    - Remove the threats
    - Disable the threats
    - Block the threats

Does cloud computing have any threats not in other computing environments?

Deployment Models

- Private Cloud
  - Owned or leased by a single organization
  - No public access
- Public Cloud
  - Owned by an organization selling cloud services
- Managed Cloud
  - Owned by a single organization
  - No public access
- Community Cloud
  - Shared by several organizations
  - Supports a specific community that has shared concerns
- Hybrid Cloud
  - Composition of 2 or more clouds
  - Enable data & application portability (e.g. cloud bursting)

Is private cloud an oxymoron?

Security Implications of the Deployment Models

Cloud Type	Manager	Owner	Location	Consumers
Private	Client or 3rd party provider	Client or 3rd party provider	On-premise or Off-premise	Trusted
Public	3rd party provider	3rd party provider	Off-premise	Untrusted
Managed	3rd party provider	3rd party provider	On-premise	Trusted or Untrusted
Community	All clients & 3rd party provider	All clients & 3rd party provider	On-premise or Off-premise	Trusted (All Clients)
Hybrid	Both client & 3rd party provider	Both client & 3rd party provider	Both On-premise & Off-premise	Trusted or Untrusted

Agenda

- **Part I - Cloud Computing (CC) Overview**
  - A Simple Definition
  - A Complete Definition
  - Security Implications
- **Part II – Is CC New?**
  - Distributed Systems Evolution
  - Security Pain Points
  - CC vs SOA
  - CC vs Outsourcing
  - CC vs SaaS
- **Part III - Cloud Computing Security**
  - Customer Security Concerns
  - How do we get attacked?
  - Security Benefits
  - Security Risks
  - Security Issues

Is CC New?

- Distributed Systems Evolution
  - Computer
  - Computer Utility (Phrase coined)
  - Computer Networking
  - LAN
  - Client/Server
  - Thin Clients
  - Internet
  - Web Applications
  - Grid Computing
  - Web Services
  - Cross Organizational Web Services
  - SaaS
  - Cloud Computing

Customer Pain Points

- P - Privacy (Confidentiality)
- A - Authorization (Authentication)
- I - Integrity (Assurance)
- N - Non-Repudiation (Accountability)

The fundamentals of security haven't changed for a long time. However, in the last few years due to viruses, worms, intrusions & DDoS attacks, another one has been added called "Assured Information Access".

CC vs SOA

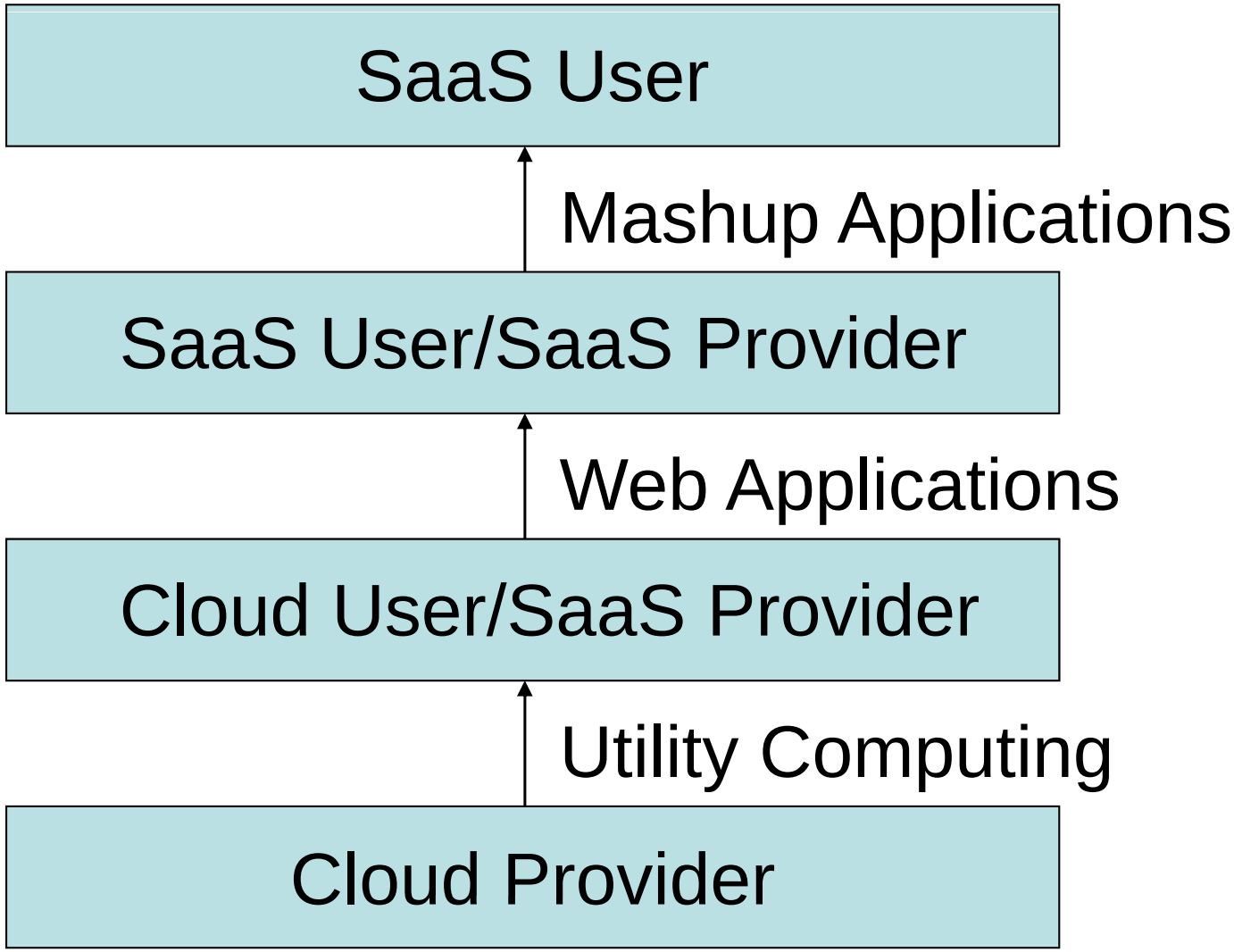
Characteristic	SOA	CC
Dynamic Linking	Yes	
Standard Protocols for Access	Yes	
Dynamic Discovery	Yes	
Relative Autonomy	Yes	
Trust Chain	Yes	
Federation	Yes	
On-demand self-service		Yes
Ubiquitous Network Access		Yes
Multi-tenancy		Yes
Rapid Elasticity		Yes
Measured Service		Yes

SOA is to cloud computing as HTML is to the internet

CC vs Outsourcing

Characteristic	**Outsourcing**	**Cloud Computing**
Standalone Computing	Yes – Move your server or hire a SP	No
Workloads	Known & controlled	Unknown & Uncontrolled
Workload Placement & Migration	Static	Dynamic – e.g. VMs migrated dynamically
Dedicated HW/SW for a customer	Yes	No
Data Location	Known	Unknown
Data replication	Not allowed	Unknown
Multi-tenancy	No	Yes
Multi-jurisdiction	No	Yes

CC vs SaaS


SaaS User
Mashup Applications
SaaS User/SaaS Provider
Web Applications
Cloud User/SaaS Provider
Utility Computing
Cloud Provider

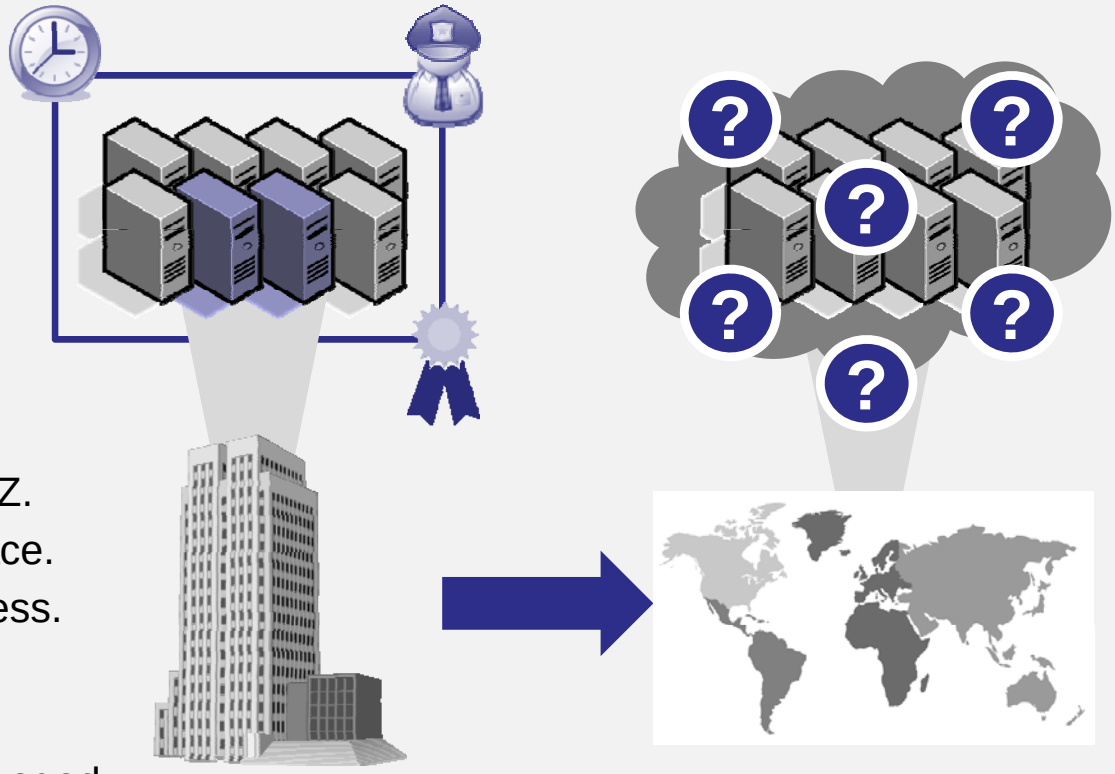
Agenda

- **Part I - Cloud Computing (CC) Overview**
  - A Simple Definition
  - A Complete Definition
  - Security Implications
- **Part II – Is CC New?**
  - Distributed Systems Evolution
  - Security Pain Points
  - CC vs SOA
  - CC vs Outsourcing
  - CC vs SaaS
- **Part III - Cloud Computing Security**
  - Customer Security Concerns
  - How do we get attacked?
  - Security Benefits
  - Security Risks
  - Security Issues

Cloud Security 101: Simple Example

TODAY

TOMORROW



We Have Control

It's located at X.
It's stored in server's Y, Z.
We have backups in place.
Our admins control access.
Our uptime is sufficient.
The auditors are happy.
Our security team is engaged.

Who Has Control?

Where is it located?
Where is it stored?
Who backs it up?
Who has access?
How resilient is it?
How do auditors observe?
How does our security team engage?

Lesson Learned: We have responded to these questions before… clouds demand **fast**, **responsive**, **agile** answers.

Categories of Cloud Computing Risks

Control

Many companies and governments are uncomfortable with the idea of their information located on systems they do not control.

Providers must offer a high degree of security transparency to help put customers at ease.

Data

Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure.

Authentication and access technologies become increasingly important.

Reliability

High availability will be a key concern. IT departments will worry about a loss of service should outages occur.

Mission critical applications may not run in the cloud without strong availability guarantees.

Compliance

Complying with SOX, HIPAA and other regulations may prohibit the use of clouds for some applications.

Comprehensive auditing capabilities are essential.

Security Management

Even the simplest of tasks may be behind layers of abstraction or performed by someone else.

Providers must supply easy controls to manage security settings for application and runtime environments.

CC Security Customer Concerns

- “I am nervous about someone else controlling my data”
- “My data is on the same disks as data from other users. If another customer’s data is raided by FBI, could mine go with it?”
- “I am not willing to say that the copy of the data in the cloud is the only copy I’ve got”
- “I am fearful of vendor lock-in”
- “I am still responsible for demonstrating compliance”
- “I don’t know where my data is stored – in which country?”
- “I don’t understand how my data is kept separate from others”
- “I don’t see how I recover my data in case of a disaster”
- “I want to investigate any illegal activity over my data”
- “I want to ensure my data is available when I need it”

Some say, Cloud security fears are overblown!

Cloud Security Breach Examples

- Google Cyber attack
  - http://googleblog.blogspot.com/2010/01/new-approach-to-china.html
- Google Doc allowed shared permission without user knowledge
  - http://www.google.com/support/forum/p/Google+Docs/thread?tid=2ef115be2ce4fd0e&hl=en
- Salesforce.com phishing attack led to leak of a customer list; subsequent attacks
  - http://voices.washingtonpost.com/securityfix/2007/11/salesforcecom_acknowledges_dat.html
- Vasrev.com Webhost hack wipes out data for 100,000 sites
  - http://www.theregister.co.uk/2009/06/08/webhost_attack/
- Twitter company files leaked in Cloud Computing security failure
  - http://www.infosecurity-us.com/view/2554/twitter-company-files-leaked-in-cloud-computing-security-failure/
- DDoS attack that downed Twitter also hit Facebook
  - http://www.computerworld.com/s/article/9136340/DDoS_attack_that_downed_Twitter_also_hit_Facebook?source=CTWNLE_nlt_security_2009-08-07

Attack Categories

- Misconfigured Programs
- Buggy Programs
  - Buffer Overflows
  - Parsing Errors
  - Formatting Errors
  - Bad input to cgi bin
- Malicious Programs
  - Trojans
  - Virus
  - Worms
  - Root kits
  - Botnets
- Unsafe Programs
- Identity Theft
- Applications
  - Cross site scripting
  - Injection flaws
  - Malicious file execution
- Eavesdropping
- Spamming
- IP Spoofing
- Phishing
- Pharming
- DoS/DDoS
- People
  - Social Engineering
  - Weak passwords
  - Sloppy Admins.

Security Benefits

- Security measures are better & cheaper due to larger scale
- Security is a market differentiator
- Information assurance is superior due to replication in multiple locations
- Cloud providers can afford to hire specialists with specific cyber security threats
- Large cloud providers can offer standardized, open interfaces to MSS (Managed Security Services)
- Cloud providers can dynamically allocate resources for filtering, traffic shaping, inspection, encryption, etc due to cloud elasticity
- Cloud computing (using virtualization) can provide pay-per-use forensic images of virtual machines which are accessible without taking infrastructure off-line, leading to less down time
- Updates can be rolled out more rapidly across a homogeneous platform
- Better Intrusion Tolerance
- Resource concentration is both a benefit & risk
  - Cheaper physical peremeterization
  - Cheaper physical access control
  - Easier/cheaper application of policy
  - Better control over management of data, patching, incidents, maintenance

Security Risks

- Lock-in (SaaS, PaaS, IaaS)
- Loss of Governance
- Compliance Challenges
- Loss of reputation due to co-tenant activities
- Cloud service termination or failure
- Cloud provider acquisition
- Supply Chain Failure
- Jurisdiction risks
- Resource Exhaustion
- Isolation Failure
- Malicious Insider
- Management Interface Compromise
- Intercepting data in transit
- Insecure/Ineffective data deletion
- DDoS
- Hardening Requirement Conflicts
- E-discovery

Security Issues

1. Data Security
2. Identity Management
3. Single Sign On
4. Applications Security
5. Secure Multi-tenancy
6. Logs & Audit Trails (Forensics)
7. Cyber Security (DPI)
8. Encryption & Key Management
9. Virtualization Security
10. Storage security
11. Information Lifecycle Management
12. Portability & interoperability
13. US Federal Specific Issues

1. Governance & Risk Management
2. Compliance
3. Vulnerability & Patch Management
4. Physical/personal Security
5. Operational security
6. Availability
7. Incident response
8. Privacy
9. Business Continuity
10. Legal Issues

Are security controls in a cloud any different than any other computing environments?

Conclusions

- Look under the hood
  - Perform onsite inspection of CP facilities whenever possible
  - Ensure CP meets all security requirements
- Be clear about your security requirements & solutions
  - Convert all/some into CP requirements
  - State integration requirements (Hybrid cloud)
  - Understand how CP will meet these
  - Be specific about your needs in the SLA
- Insider threat is a significant concern
  - Robust compartmentalization of job duties
  - Privileged user access control
  - Malicious tenants
- Ensure discovery & forensics requirements are met
- Understand the handling of transitive trust
  - What suppliers does the cloud provider depend on? (Recursive)
- Evolving convergence of physical & IT security introduce new risks
- Shop around for multiple CP's (inter cloud integration)
- Have open and frequent discussion with CP

Cloud computing provides new economies for information technologies as well as new challenges. Properly constructed, it can be more secure than traditional IT infrastructure, but that construction requires the use of strong, integrated and usable security mechanisms.